УДК 811.161.1’23’37: 343.21

10.00.00 Филологические науки

НЕКОТОРЫЕ СПОСОБЫ СОКРЫТИЯ ИНФОРМАЦИИ В УГОЛОВНОМ ДИСКУРСЕ И ПРИМЕНЕНИЕ АСК-АНАЛИЗА

Зубков Евгений Анатольевич
к.ф.н., доцент
v.zubkova@upcpoczta.pl
Университет Яна Кохановского, г. Кельце, Польша (Uniwersytet Jana Kochanowskiego w Kielcach, Instytut Filologii Obcych, ul. Świętokrzyska 21D, 25-406 Kielce, Polska)

Целью представленной статьи является рассмотрение возможностей применения АСК-анализа и системы «Эйдос» для русского уголовного дискурса в его различных аспектах. В статье показаны некоторые способы передачи информации посвященным с одновременным сокрытием ее от непосвященных, на их фоне выделяется т.н. «криптосистема с открытым ключом» и доказывается ее устойчивость относительно современных методов криптоанализа. Такой «криптосистемой с открытым ключом» является Новый Воровской Закон. Эта криптосистема работает на основе асимметричных функций, основывается на «шести требованиях Керкгоффса», использует открытые случайные ключи и «секретные лазейки» (алгоритм RSA и схему обмена ключами Диффи-Хеллмана-Меркле). Термины используются согласно современному уровню научных знаний, в русском уголовном дискурсе математический принцип работы такой системы носит название «Воровская Идея». Для такой системы доказывается неполная функциональность классического контент-анализа, успешно используемого для иных упоминаемых способов сокрытия информации. Одновременно с этим высказываются предположения относительно дальнейших модификаций системы «Эйдос» для успешного ее использования относительно такой «криптосистемы с открытым ключом». В статье мы также сосредотачиваемся на невозможности восприятия Нового Воровского Закона как юридического факта

Ключевые слова: «КРИПТОСИСТЕМА С ОТКРЫТЫМ КЛЮЧОМ», «НОВЫЙ ВОРОВСКОЙ ЗАКОН», АСИММЕТРИЧНЫЕ ФУНКЦИИ, СИСТЕМА «ЭЙДОС»

UDC 811.161.1’23’37: 343.21

Philology

SOME WAYS TO HIDE TRANSFERRED INFORMATION IN RUSSIAN CRIMINAL DISCOURSE VS. COMPUTERIZED SYSTEM-COGNITIVE ANALYSIS

Zubkov Evgeniy Anatolyevich
Cand.Philol.Sci., assistant professor
v.zubkova@upcpoczta.pl
Jan Kochanowski University in Kielce, Poland

The article focuses on the possibilities of application of the Computerized System-Cognitive Analysis (CSC-Analysis) and the “Eidos” Intellectual System for the Russian criminal discourse in its various aspects. In the work, the author shows some simultaneous ways to transfer information to the Initiated and hide it from others. The author distinguishes such public-key cryptography system from their background and proves its resistivity to modern cryptography methods. The New Thieves’ (Felons’) Law as a public-key cryptography system is based on asymmetric functions, works according to the Kerckhoffs’s law, uses accidental public keys and “knapsack trapdoors” (RSA algorithm and the Diffie-Hellman-Merkle Key-Exchange Protocol). The terms are used in this paper according to modern level of scientific knowledge. In the Russian criminal discourse, the mathematical principle for such system is called “The Russian Felony Idea”. A classical content-analysis applicable for other ways to hide transferred information in this paper is inconsistent for such cryptosystem. The author also suggests some ideas concerning further modifications of the “Eidos” Intellectual System to apply it sufficiently for such public-key cryptography system. Moreover, the author focuses on the problem of the New Thieves’ (Felons’) Law as Fait juridique

Keywords: PUBLIC-KEY CRYPTOGRAPHY SYSTEM, NEW THIEVES’ (FELONS’) LAW, ASYMMETRIC FUNCTIONS, “EIDOS” INTELLECTUAL SYSTEM

Взгляды на термин «дискурс» разнообразны и зависят от используемой методологии. Представленная статья не имеет целью

опровергать или подтверждать какой-либо из них. Автором представленной статьи термин «дискурс» применяется согласно функционально-прагматической модели лингвосемиотического опыта О.В. Лещака и понимается как «(...) пространственно-временной и информационный континуум, который сосредотачивается вокруг текста (или набора текстов) в процессе его (их) создания или воспроизведения по определенным принципам лингвосемиотической системы (кода) в границах определенного функционального типа деятельности, основанной на опыте (...)» [3: 34]. Словоупотребление «уголовный» в русском языке имеет множество смыслов, в представленном исследовании мы рассматриваем его с точки зрения *реляции с окружением при крайней (профессиональной) степени вовлеченности в деятельность, рассматриваемую как преступная относительно закона в любом временном отрезке, при наличии веры индивида в то, что подобная деятельность является правильной с любой точки зрения.* Вера индивида (точнее определенный «символ веры» с точки зрения концепции этногенеза Л.Н. Гумилева) крайне важна для целей представленного исследования, поскольку позволяет показать один из способов передачи информации посвященным и одновременного сокрытия ее от непосвященных и доказать его устойчивость относительно современных методов криптоанализа. Кроме того, необходимо упомянуть, что исследуемый способ передачи информации *не существует как юридический факт и является т.н. «отсутствующей структурой»* согласно концепции У. Эко: «(...) за самыми привычными навыками нашего поведения в глубине скрывается схема поведения наших предков (...) всякое гипостазирование структурального разума имеет свои пределы, положенные ему реальностью серийной техники, модифицирующей пресловутые вечные константы (...). Серийность не будет выглядеть тогда простым отрицанием структуры, но сама окажется структурой (...)»[8: 410].

Заметим, что предлагаемая для исследования русского уголовного дискурса модель является синтезом взглядов вышеупомянутых авторов, а возможность ее применения и «работоспособность» были уже доказаны [1]. Целью данной статьи является исследование т.н. «криптосистемы с открытым ключом» (Нового Воровского Закона), выделение основных его черт на фоне иных способов передачи и сокрытия информации, а также конфронтации с возможностями уже имеющегося метода (АСК-анализа), который доказал свою применимость и работоспособность в иных областях науки и техники. Учитывая новизну и актуальность нашей статьи, ссылки нами будут даны лишь в меру их релевантности во избежание повторения широкоизвестной информации. Поэтому, после введения читателя в суть проблемы, мы сразу же перейдем непосредственно к теме исследования.

Способы сокрытия информации условно принято разделять на стеганографию и криптографию, поскольку в ряде случаев они друг друга дополняют. В криптографии выделяют два основные типа: шифрование и кодирование, которые также могут использоваться одновременно и также дополнять друг друга. Можно говорить о перестановке или замене (слов или букв), даже о перестановке в одной букве с развитием компьтерной техники. Необходимо заметить, что практически все они на настоящий момент неустойчивы к декодированию и дешифрованию, если это действительно нужно сотрудникам правохранительных органов. К наиболее известным, и еще распространенным в современности, мы можем отнести:

1) «Треугольник» – «Письмо, складываемое треугольником таким образом, что на неисписанной его части остается место для адреса. Этот способ применялся еще в XIX в., главным образом крестьянами и солдатами. В советское время им пользуются этапируемые заключенные: треугольник без марки выбрасывают через отверстие уборной; это

нетрудно в товарном вагоне, труднее в столыпинском. Обычно треугольник подбирает железнодорожный обходчик и затем опускает в почтовый ящик. Огромное большинство треугольников попадало по адресу, даже в годы сталинских чисток. Примеч. во время 2-й мировой войны советские солдаты, за неимением конвертов, посылали домой треугольники»[6 (2: 411)]. Автор представленного исследования высказывал предположение, что причиной доставления таких писем по адресу была «биографическая степень приближения к предмету» согласно концепции Л.Н. Гумилева [1: 283-284], т.е. биография самого И.В. Сталина, о чем упоминает Лев Троцкий [7: 309]. В настоящее время более фреквентны словоупотребления «ксивы», «малявы», «кони» и т.д. (в зависимости от степени открытости или закрытости документа и способа его передачи), с элементами кодирования или шифрования. Меняются названия и формы, суть способа остается та же. *Уголовная наказуемость зависит не от степени стойкости, а от функциональной прагматики*.

2) «Морзянка», в настоящее время называемая «тукованием»: «Тюремная морзянка заменяет точку одним ударом (в стену соседней камеры), а тире – двумя быстрыми. Очень часто применяется другая система, где первый удар обозначает ряд, а второй – букву в ряду. После каждого переданного слова передающий царапает стену и ожидает подтверждения принимающего. Если тот подтвердит (один удар), тогда передается следующее слово. В противном случае вновь передается последнее слово. Три удара обозначают ‘повтори’. Три удара или больше означают, что передающий ошибся и повторит переданное» [6 (1: 222-223)]. Можно при «морзянке» («туковании») пользоваться общераспространенным кодом Вейзля-Морзе-Герке; можно применить т.н. «шифр Цезаря» – сдвиг букв алфавита на несколько позиций, или «штакетник» – *симметричное* переставление сразу нескольких букв в алфавите. Можно использовать «сталаговскую морзянку» (хотя название

не соответствует месту применения), по своему принципу действия повторяющую «малый квадрат» или даже «большой квадрат» при наличии записей (шифр Альберти-Вижинера). Администрации (У)ФСИНа применение криптографии неинтересно с точки зрения, опять же, функциональной прагматики, поскольку имеются иные способы воздействия.

3) С чисто теоретической точки зрения, интересны т.н. условные коды, причем старшие их версии (особенно «байковые лозунги»), по мнению автора, имеют большую стойкость, чем современные. Например: «Лозунгом обычно служит как будто безотносительно сказанное замечание о ‘погоде’ смотря по времени и обстоятельствам. Слово ‘погода’, сказанное одним, непременно вызывает подходящий ответ другого. Таким образом, если в ответ на ‘погоду’ скажется ‘серо’, то это означает, что пока еще неизвестно, как пойдет дело. ‘Мокро’ и ‘вода’ выражают полную опасность. ‘Снег’ и ‘дождь’ смотря по времени года служат не лозунгом опасности, но неудачи, а ‘ясно’ – показывает совершенно противоположное. Иногда же и ‘погода’ служит ответом на ‘погоду’, сказанную проходящим и осведомляющимся сообщником, и в этом последнем случае, смотря по тону, каким была произнесена ‘погода’, она служит ответом на удачу или неудачу дела» [2 (1: 581)].

Ранее было высказано предположение, что «(...) в случае ‘байкового лозунга’ ‘погода’ мы имеем дело с омофоническим кодом замены, однако рассматривать этот код только в таком качестве будет не совсем правомерно. Автор исследования склонен полагать, что в данном случае можно говорить о культурном коде с элементами омофонического кода замены, поскольку зачастую *важным бывает ‘тон, каким была произнесена ‘погода’*» [1: 287]. В данной связи уместно замечание, что *очень трудно признать интонацию противоправным действием*. Если говорить о современных условных кодах, особенно в устной форме, то

может наблюдаться «(...) омофонический код замены условных слов, однако остальная часть сообщения не кодируется, или же кодировка является *плавающей* (т.е. *случайной* в терминах криптоанализа)» [1: 287]. Речь идет о условном назывании предмета противоправной сделки отвлеченным термином с дальнейшим «последовательным развертыванием темы» («концентрическим развертыванием» согласно Б.А. Ларину, доказательство различия для темы данного исследования нерелевантно). Имеется в виду языковая игра собеседников с опорой на условленное ранее называние, что дает необходимый элемент случайности, но значительно ограничивает т.н. «массив». Расширение «массива» может привести к непониманию между собеседниками и смещению референциальности. Для целей представленного исследования нерелевантно углубление в классический контент-анализ, поскольку «(...) если разговор прослушивается работниками правохранительных органов, то для этого должны иметься основания. С другой стороны, при данном виде кодирования сообщения в случае неизвестности говорящих сотрудникам правохранительных органов, такой омофонический код замены может давать сравнительную устойчивость к обнаружению устаревшими программами типа ‘Эшелон’, *но не устойчивость к декодированию, если соответствующим службам это действительно нужно. Данный вид кодировки рассчитан на двух пользователей и не предназначен для более широкого распространения*» [1: 290]. Если попытаться экстраполировать идею «законника» как «человека-книги» на индейцев чокто во время Первой мировой войны и радистов-навахо во время Второй мировой войны, то мы не заметим у «законных воров» уникальной грамматики и в некотором роде фонетики, являвшихся основными средствами защиты передаваемого сообщения в то время, лишь слабую сторону – попадание носителя кода в руки противника. Как известно, человеческое тело подвержено действию гравитации, инфекции,

психотропных средств и т.д., но Воровской Закон не был раскодирован до настоящего времени, были замечены лишь какие-то его проявления с установлением очень слабых системных зависимостей. С точки зрения Л.Н. Гумилева мы можем говорить о «силе вещей», с точки зрения АСК-анализа – о научном прогрессе.

Каждый из упомянутых выше способов передачи информации посвященным и сокрытия от непосвященных находится в иной области знания и системно исследуется различным инструментарием, что позволяло исследователям игнорировать факты и системные зависимости («характеристики связей») в силу ряда причин. Для координации исследований из разных областей знания и управления ими нужна проверенная система, которая бы совмещала не только исследование свершившихся фактов, но и позволяла бы прогнозировать дальнейшее развитие событий [5]. Как автор представленного исследования упоминал ранее, такой системой могут являться версии системы «Эйдос» Е.В. Луценко на основе методологии АСК-анализа [1: 28, 317].

Однако следует заметить, что в настоящий момент *даже научный прогресс не в состоянии сделать (Новый) Воровской Закон юридическим фактом и привести к тому, что только за принадлежность* к «законным ворам» можно быть приговоренным к лишению свободы. Вызвано это следующими причинами, *устранить которые в практическом применении в ближайшие несколько десятков лет не представляется возможным (если когда-либо вообще)*, однако можно постулировать теоретически и создать работоспособную модель при помощи АСК-анализа. Рассмотрим эти основные проблемы:

1. Не вызывает сомнения, что даже стереотип реакций индивида (не говоря уже о алгоритме поведения) может резко нарушаться под влиянием экстремальных ситуаций, причем реакции типа борьбы и бегства могут включать в себя также довольно плохо изученные оцепенение и

самообман, что может приводить к искажению действительности. Опять же, может возникнуть проблема понимания действительности и ее дефиниции. Кроме того, противопоставление и единство индивида с окружением, в том числе в преступной (уголовной, уголовно-наказуемой) деятельности являются процессами разной интенсивности. «(...) Нельзя утверждать, что главной детерминантой будет выбор ‘преступление – непреступление’ в чистом виде, будет наблюдаться ряд иных дихотомических противопоставлений на основе ‘разности потенциалов’» [1: 25]. Эта проблема была уже решена при помощи АСК-анализа путем создания работоспособной модели [4: 41-42], и при введении соответствующих данных, что предусматривает дополнительное финансирование, будет дальше успешно решаться на практике.

2. Теперь непосредственно перейдем к теме исследования и проблеме, которая даже при значительном увеличении финансирования может решаться лишь теоретически, т.е. к сути «Воровской Идеи». Автор представленного исследования указывал на полный авторефлексии взгляд Л.Н. Гумилева о связях в системе, которые могут быть как положительными, так и отрицательными, а также смену знака подсистемы даже на протяжении жизни особи [1: 41]. Эта проблема решается в математике при помощи нелинейных функций, но по отношению к Новому Воровскому Закону, по мнению автора исследования, такое решение неприменимо.

Новый Воровской Закон является синтезом ряда религиозно-правовых систем, которые в настоящее время совершенно легальны. *Теоретически находясь в стадии гомеостаза, Воровской Закон постоянно меняется в связи с развитием научных знаний относительно этих систем*. Вызвано это, в упрощении, биективной функцией, и сюръекция при трансформации Старого Воровского Закона в Новый Воровской Закон заставляет нас обратить внимание на произвольное непрерывное

сюръективное отображение топологических пространств. Здесь множество с дополнительной структурой определенного типа может быть, конечно же, определено предбазой. Эта проблема решается без существенных модификаций версий системы «Эйдос», даже при недостатке исходных данных. Однако остается ряд трудно решаемых проблем. *Первой из них является ответ на вопрос, имеем ли мы дело с (пред)базой, или же псевдобазой*. Как упоминалось выше, был установлен определенный код, «Код Божий» [1: 315] для адептов «Воровской Идеи» в пространственно-временном и информационном континууме согласно функционально-прагматической модели лингвосемиотического опыта О.В. Лещака. Автор представленной статьи склонен полагать, что *под натуральные явления природы была подведена достаточно логичная мифоидеологическая основа*, в настоящее время называемая «Воровской Идеей». Более того, *исследуемая система (дискретная антисистема согласно концепции этногенеза Л.Н. Гумилева) дискретна, сигнал длителен (несколько столетий), доверительный интервал неточен, а для дискретных систем с длительностью сигнала, по мнению автора, являющегося по образованию филологом, подходит точечная выборка (в языкознании на основе словарей и источников, также неполных) с применением адекватной модели реконструкции*. Было постулировано, на основе современного состояния науки и доступа к информации, что Новый Воровской Закон является «криптосистемой с открытым ключом» в современных терминах, основывается на «шести требованиях Керкгоффса», «система в руках врага» (или же «враг знает систему» Клода Шеннона), работает на основе односторонних функций модулярной арифметики (*асимметричных функций*), и использует открытые случайные ключи и «секретные лазейки» (алгоритм RSA и схему обмена ключами Диффи-Хеллмана-Меркле) [1: 292-298]. Как уже упоминалось выше, версии системы «Эйдос» теоретически способны решить все эти проблемы, но тогда для

каждой процедуры и подпроцедуры необходимо высчитывать алгоритмы асимметричных функций, для каждого из модулей, что предусматривает наличие огромного количества вводимых данных (в том числе на «биографической степени приближения» исследуемых, что практически невозможно) и квантовых компьютеров.

На практике такие исследования не создадут юридического прецедента, когда только за принадлежность к «законным ворам» будут приговаривать к лишению свободы, поскольку в правовом демократическом государстве не лишают свободы за идеи, а лишь за уголовно-наказуемые деяния. *Воровской Закон не станет юридическим фактом в обозримом будущем*.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Зубков Е.А., Иносказание в русском уголовном дискурсе. «Масти», «Понятия», «Воровской Закон». Кельце: Изд. Университета им. Яна Кохановского 2014. – 397 с.
2. Крестовский В.В., *Петербургские трущобы (книга о сытых и голодных)* в 2-х томах. Л.(СПб): Изд. Художественная литература 1990. Т. 1 – 704 с., Т. 2 – 800 с.
3. Leszczak O., Lingwosemiotyka kultury. Funkcjonalno-pragmatyczna teoria dyskursu. Toruń: Wyd. Adam Marszałek 2010. – 415 с.
4. Луценко Е.В. Применение АСК-анализа и интеллектуальной системы "Эйдос" для решения в общем виде задачи идентификации литературных источников и авторов по стандартным, нестандартным и некорректным библиографическим описаниям / Е.В. Луценко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №09(103). С. 498 – 544. – IDA [article ID]: 1031409032. – Режим доступа: http://ej.kubagro.ru/2014/09/pdf/32.pdf, 2,938 у.п.л.
5. Луценко Е.В. Синтез, верификация и исследование на устойчивость системно-когнитивной модели перерабатывающего комплекса региона / Е.В. Луценко, В.И. Лойко, Т.П. Барановская // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №07(101). С. 305 – 333. – IDA [article ID]: 1011407016. – Режим доступа: http://ej.kubagro.ru/2014/07/pdf/16.pdf, 1,812 у.п.л.
6. Росси Ж., Справочник по ГУЛАГу. В 2-х частях. Изд. 2-е, дополненное. М.: Просвет 1991. Ч. 1 – 269 с., Ч. 2 – 284 с.
7. Троцкий Л., Сталин. // История в лицах. Диктаторы. М.: Интер Дайджест 1995. – 368 с.
8. Эко У., Отсутствующая структура. Введение в семиологию. СПб: Симпозиум 2004. – 544 с.

References

1. Zubkov E.A., Inoskazanie v russkom ugolovnom diskurse. «Masti», «Ponjatija», «Vorovskoj Zakon». Kel'ce: Izd. Universiteta im. Jana Kohanovskogo 2014. – 397 s.

2. Krestovskij V.V., Peterburgskie trushhoby (kniga o sytyh i golodnyh) v 2-h tomah. L.(SPb): Izd. Hudozhestvennaja literatura 1990. T. 1 – 704 s., T. 2 – 800 s.

3. Leshhak O., Lingvosjemiotyka kul'tury. Funkcional'no-pragmatychna tjeorija dyskursu. Torun': Vyd. Adam Marshaljek 2010. – 415 s.

4. Lucenko E.V. Primenenie ASK-analiza i intellektual'noj sistemy "Jejdos" dlja reshenija v obshhem vide zadachi identifikacii literaturnyh istochnikov i avtorov po standartnym, nestandartnym i nekorrektnym bibliograficheskim opisanijam / E.V. Lucenko // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2014. – №09(103). S. 498 – 544. – IDA [article ID]: 1031409032. – Rezhim dostupa: http://ej.kubagro.ru/2014/09/pdf/32.pdf, 2,938 u.p.l.

5. Lucenko E.V. Sintez, verifikacija i issledovanie na ustojchivost' sistemno-kognitivnoj modeli pererabatyvajushhego kompleksa regiona / E.V. Lucenko, V.I. Lojko, T.P. Baranovskaja // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2014. – №07(101). S. 305 – 333. – IDA [article ID]: 1011407016. – Rezhim dostupa: http://ej.kubagro.ru/2014/07/pdf/16.pdf, 1,812 u.p.l.

6. Rossi Zh., Spravochnik po GULAGu. V 2-h chastjah. Izd. 2-e, dopolnennoe. M.: Prosvet 1991. Ch. 1 – 269 s., Ch. 2 – 284 s.

7. Trockij L., Stalin. // Istorija v licah. Diktatory. M.: Inter Dajdzhest 1995. – 368 s.

8. Jeko U., Otsutstvujushhaja struktura. Vvedenie v semiologiju. SPb: Simpozium 2004. – 544 s.